一种抗几何旋转攻击零水印算法 *

刘万军，孙思宇†，曲海成，冯　琳，何牧泽

(辽宁工程技术大学 软件学院，辽宁 葫芦岛 125105)

摘　要：为了解决零水印算法存在抗几何攻击能力弱的问题，提出了一种抗几何旋转攻击的零水印算法。首先根据尺度不变特征变换(SIFT)旋转校正后图像像素失真情况，在中心地带确定像素近似无损的安全区域；其次将该区域进行二级冗余离散小波变换提取低频区域，对该低频区域进行分块并提取每个块的最大奇异值，同时利用每块最大奇异值构建过渡矩阵；然后通过比较过渡矩阵的每个元素值与其均值关系构造特征矩阵；最后将加密后的水印图像与特征矩阵共同构建零水印。实验结果表明，与仅利用 SIFT 校正算法相比，抗旋转攻击鲁棒性平均提高了 13.26%，与 GH 旋转矩和伪 Zernike 正交矩算法相比，抗旋转攻击鲁棒性分别提高了 1.1%和 0.94%；对常规攻击、缩放攻击和循环平移以及小范围的剪切攻击均具有较强鲁棒性。

关键词：尺度不变特征变换；内接正方形区域；冗余离散小波；Arnold；特征矩阵；奇异值分解；抗几何攻击

中图分类号：TP309　　doi: 10.3969/j.issn.1001-3695.2018.04.0212

Anti-geometric rotation attack zero watermarking algorithm

Liu Wanjun, Sun Siyu†, Qu Haicheng, Feng Lin, He Muze

(*College of Software Liaoning Technical University*, *Huludao Liaoning* 125105, *China*)

Abstract: To solve the problems of the zero-watermarking algorithms with weak against geometric attack, this paper proposed a zero-watermarking algorithm against geometric rotation attack. Firstly, the algorithm determined the near-destructive maximum inscribed square region with approximately pixels lossless in the center area, according to the pixel distortion of the image of the scale-invariant feature transform (SIFT) rotation correction. Then, the square region performed two-level redundant discrete wavelet transformation and extracted the low-frequency region. What's more, it extracted the largest singular value of each block to construct a transition matrix into block processing from the low-frequency area. Next, to obtain a characteristic matrix, it compared the value of each element in the transition matrix with its average value. Finally, it used the watermark image and constructed the characteristic matrix a zero watermark. The experimental results show that compared with the only rotation correction algorithm of SIFT, the robustness against rotation attack is up by an average of 13.26%. Compare with the rotation corrections algorithms of the GH rotation moment and pseudo-Zernike orthogonal moment, the anti-rotation attack robustness is up by 1.1% and 0.94% respectively. Also, it has a good effect on common conventional attacks, scaling attacks, cyclic translation and small-scale shear attacks.

Key words: scale-invariant feature transform; in-square square region; redundant discrete wavelet; Arnold; eigen-matrix; singular value decomposition (SVD); anti-geometric attack

0　引言

零水印[1]的思想，主要通过利用原始载体图像的内部特征进行构造，保证了原始载体图像完整性，打破了传统水印算法鲁棒性与不可见性之间的矛盾。一直以来，由于几何攻击会破坏载体图像与水印的同步性，使得水印无法正确提取。相比传统数字水印，零水印则能更好地克服几何攻击。为了有效提高图像水印算法抗几何攻击能力，基于图像特征点的第 2 代图像水印技术得到外界了广泛关注[2]。文献[3~5]利用图像尺度不变特征变换（scale-invariant feature transform，SIFT）匹配攻击前后的特征点作为模板来校正图像的几何失真，从而达到同步水印信息抵抗旋转攻击的目的，但均没有考虑到旋转攻击带来的

收稿日期：2018-04-02；**修回日期：**2018-05-19　**基金项目：**国家自然科学基金资助项目（61172144）；辽宁省自然科学基金资助项目（20170540426）；辽宁省教育厅一般项目（LJYL049）

作者简介：刘万军（1959-），男，辽宁北镇人，教授，硕士，主要研究方向为数字图像处理、运动目标跟踪；孙思宇（1993-），女（通信作者），硕士研究生，主要研究方向为数字图像处理、人工智能（international_sun@163.com）；曲海成（1981-），男，山东烟台人，副教授，博士，主要研究方向为遥感图像处理；冯琳（1993-），男，硕士研究生，主要方向为数字图像处理；何牧泽（1996-），男，辽宁阜新人，学士，主要研究方向为数字图像处理.

像素缺失问题。贾超等人[6]则提出了基于改进 SIFT 的抗几何攻击的水印算法，将旋转不变纹理特征信息融合到传统 SIFT 特征向量当中，进而提高了匹配进度。Zhang 等人[7]通过使用加速鲁棒特征（speeded-up robust features，SURF）和 RANSAC 算法整体提高了提取特征点的质量，再使用放射变换来提高校正的精度，其本质是优化了特征点检测，并没有考虑旋转攻击带来的像素值缺失导致提取的水印缺失问题。

虽然特征点匹配算法能够有效抵抗旋转攻击，但是随着旋转角度的增加，算法的鲁棒性也将越来越差。其中，最直接原因是旋转攻击不仅将元素位置进行改变，同样也会损失一定的像素值，造成旋转校正后的图像一部分的像素缺失。因此针对该现象，传统水印算法也通过构建不变域或不变矩的方法构造。Jia 等人[8]提出了基于局部信息图像归一化的抗几何攻击数字水印算法，主要通过选择一个旋转校正后不会带来影响局部的 GH 区域进行水印的嵌入与提取，但随着嵌入水印区域的缩小，算法的容量也会减少。此外，朱丹丹等人[9]将水印信息嵌入到载体图像低频的伪 Zernike 矩幅值当中，提高了水印鲁棒性。陈青等人[10]运用 Harris 算法提取载体图像特征点，并构建局部特征区域，通过量化调制伪 Zernike 矩幅值将水印信息嵌入到局部特征区域，利用伪 Zernike 矩的相位信息对受到旋转攻击的图像进行几何校正，能够有效地抵抗旋转攻击。

由文献[8,10]可得，通过寻找载体图像不会因受到旋转攻击而像素值失真的部分来完成水印的嵌入，可有效地提高 SIFT 几何校正水印算法的鲁棒性。通过多次实验，若在载体图像的中心点处附近选取像素缺损范围最小且校正后图像的内接正方形区进行零水印的构建与水印的提取，可以减少像素的缺损现象。此外，为了弥补因减少载体图像面积所带来的嵌入容量减少问题，所以本文选用冗余离散小波变换(RDWT)在不减小分解后子图大小特性的前提下提取图像的稳定低频区域[11]，并提取图像块的最大奇异值构造特征矩阵，与加密后的水印信息共同构建零水印。

1　构建区域的选择

1.1　尺度不变特征变换

尺度不变特征变换(SIFT)是用来检测图像局部特征的一种算法，在多尺度空间[12]提取尺度、位置、旋转不变量中特征点的过程。因 SIFT 特征点算子具有尺度不变性和可改变图像旋转角度或亮度等特性，所以 SIFT 变换的本质内容是构建尺度空间并搜索具备高鲁棒性的图像突出的信息特征点，且这些特征点不会因光照强度改变、遮挡等问题出现而消失。即在尺度空间检测极值点，然后对极值点进行筛选，提取在每个稳定特征点周围的图像局部特性形成局部描述符。通过欧式距离实现匹配，得到匹配后特征点的尺度、位置、方向和描述子，完成图像的几何校正过程。

1.1.1 尺度空间的构建

尺度空间的作用在于模拟图像数据的多尺度特征。高斯卷积核是实现尺度变换的唯一线性核。用函数 $L(x,y,\sigma)$ 描述图像的尺度空间，是图像 $I(x,y)$ 和尺度可变换的高斯函数 $G(x,y,\sigma)$ 卷积的结果。即高斯函数 G 对图像 I 的模糊函数见式(1) (2)。

$$L(x,y,\sigma)=G(x,y,\sigma)\otimes I(x,y) \tag{1}$$

$$G(x,y,\sigma)=\frac{1}{2\pi\sigma^2}e^{-(x^2+y^2)/2\sigma^2} \tag{2}$$

其中：$\otimes$ 表示卷积；(x,y) 表示空间坐标，表示图像的位置；σ 表示尺度空间因子，其值的大小与图像 I 被平滑的程度成正比。当图像被平滑得越多，则图像呈现得越模糊，相应的尺度越大。

DoG(高斯差分尺度空间)是通过将高斯金字塔中每一组中上下相邻的两层高斯尺度图像进行相减而得。高斯差分函数见式(3)。

$$\begin{aligned}D(x,y,\sigma)&=(G(x,y,k\sigma)-G(x,y,\sigma))\otimes I(x,y)\\&=L(x,y,k\sigma)-L(x,y,\sigma)\end{aligned} \tag{3}$$

1.1.2 关键点方向参数确定及特征点描述算子确定

关键点方向参数的确定主要利用边缘强度 M 和边缘方向 θ，实现方式如式(4)所示。

$$\begin{aligned}M_{SIFT}(x,y)&=\sqrt{(L(x+1,y)-L(x-1,y))^2+(L(x,y+1)-L(x,y-1))^2}\\\theta_{SIFT}(x,y)&=\tan^{-1}\frac{(L(x,y+1)-L(x,y-1))}{(L(x+1,y)-L(x-1,y))}\end{aligned} \tag{4}$$

其中：L 表示关键点所在尺度。通过利用直方图统计邻域内像素的梯度方向，特征点直方图的峰值可表示该特征向量的局部方向，再计算特征的主方向，保证描述符具备旋转不变性。特征向量的生成过程如图 1 所示。图中黑点表示某特征关键点，每个方块小格表示关键点邻近点的一个像素，像素的梯度方向为箭头所指方向，梯度的模即为箭头的长度。

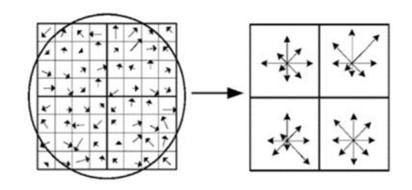


图 1　特征点邻域梯度信息与特征向量

1.1.3 SIFT 特征点匹配校正

a) SIFT 特征匹配是凭借特征点之间的相似度量所进行的过程。先通过计算两幅图像 SIFT 特征点描述符的欧氏距离对 SIFT 特征向量进行匹配，在获取特征向量值后，采用优先 K-D 树进行优先搜索查找每个特征点的近似最近邻特征点。检测两个特征点，若较短的距离除以次短的距离不高于某个上限值，则接受此对匹配点。通过更改这个上限值，可控制特征匹配点的数量。上限值变大时匹配点数目增多，产生较多的误匹配点，匹配稳定性变差，反之同理。通过大量实验得出，当比例阈值在[0.4,0.6]时，匹配效果理想。

b) SIFT 是一种基于空间的对图像旋转、缩放和平移保持不

变性的图像局部特征描述算子。若在中心区域存在两个点 A、B，若图像旋转 α 角度，则认为 A、B 两点均旋转相同角度，即只需判定两对特征点之间连线的夹角实现旋转校正（其中，*oo'*为两图像中心点的连线）。提取并匹配旋转攻击前后两幅图像 SIFT 特征点，利用匹配特征点的位置信息进行旋转校正。假设原始载体图像中的两个特征点坐标分别为 (x_i, y_i) 和 (x_j, y_j)，经过旋转攻击后的两个特征点的坐标分别为 (x_i', y_i') 和 (x_j', y_j')，旋转角度图如图 2 所示。

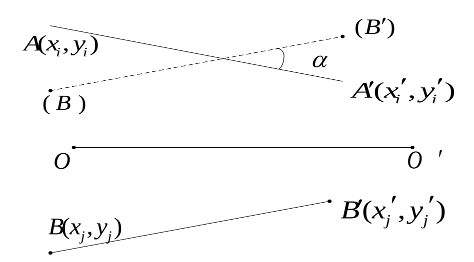


图 2　特征点旋转示意图

a)使用两对特征点之间连线的水平夹角的变化矫正图像，利用公式(5)求出每组的旋转角度。

$$\Delta\alpha = \arctan\frac{y_i - y_j}{x_i - x_j} - \arctan\frac{y_i' - y_j'}{x_i' - x_j'} \tag{5}$$

b)将所有分组求出的旋转角度进行 *n* 等分，利用直方图求出各个区间的频数 *m* 及相应的旋转角度 *p*，找到最大频数 m_{max}，求出频数相对较大的旋转角度 *pm*，筛选在[*pm*-1,*pm*+1]内的旋转角度，得出筛选后旋转角度的平均值即为旋转校正角度值，见式(6)(7)。

$$pm = \frac{\sum_{i=1}^{num}(p(i) \times m(i))}{\sum_{i=1}^{num} m(i)} \tag{6}$$

$$\alpha = \frac{1}{N}\sum_{i=1}^{N}\Delta\alpha_i \tag{7}$$

其中：*num* 表示频数 *m*(*i*)大于 0.85×m_{max}[*pm*-1，*pm*+1]区间内的旋转角度；N 表示筛选后的旋转角度个数。

1.2　内接正方形安全区域的确定

1.2.1 旋转校正后像素缺损的规律

SIFT 载体图像在经过 1°~359°的旋转过程中边缘信息会有程度不一的像素缺损，且经过旋转校正后的载体图像也无法弥补之前缺失的像素部分。原始载体图像和受到不同角度旋转攻击的效果如图 3 所示，仅利用 SIFT 算法校正后的效果如图 4 所示，不同角度旋转攻击后的旋转校正结果以及缺损情况见表 1。

由图 4 可得如下启发：

a)无论经过任何角度的旋转，原始载体图像的中心地带总有一部分像素数据不会出现缺损现象；

b)载体图像经过 15°的旋转攻击效果图与经过 75°的旋转攻击效果图所缺损的像素面积相同；

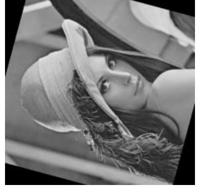
c)当载体图像受到 45°、135°、225°和 315°时，载体图像所损失的面积达到极值且相同（NC 值）。


(a) 原始载体图像


(b) 旋转 5°


(c)旋转 15°


(d) 旋转 45°


(e) 旋转 75°


(f) 旋转 125°

图 3　原始图像和受到不同角度旋转攻击后的图像


(a) 校正旋转 5°


(b) 校正旋转 15°


(c) 校正旋转 45°


(d)校正旋转 75°


(e)校正旋转 125°

图 4　仅利用 SIFT 旋转校正后的图像

表 1　旋转攻击后旋转校正结果及缺损情况

旋转角度(°)	校正参数	Lena	Boat	Bridge	图像是否有损失
5	-5	-4.9972	-4.9863	-5.0245	有
10	-10	-10.0120	-9.9973	-9.9876	有
15	-15	-15.0010	-14.9968	-14.9988	有
20	-20	-19.9738	-19.9743	-19.9933	有
30	-30	-30.0118	-30.0378	-29.9832	有
45	-45	-45.1030	-44.9863	-44.9899	有
55	-55	-55.0100	-54.9871	-54.9921	有
75	-75	-75.0914	-74.9789	-74.9863	有

由此可得，图像若在经过 0~360°各个角度的攻击下，所损失的面积以及具体的位置将会出现周期性，即可得 $(45k)° \sim (45(k+1))°, (k = 0,1...7)$ 规律，呈 45°为一周期变化。特别地，当载体图像受到 45°、135°、225°和 315°的旋转攻击时，损失的面积最大，且损失的位置相同，因此在经过旋转校正后的 45°图像中找到内接的正方形，其他角度同理可

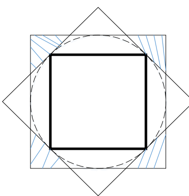
得。

因此，本文在 SIFT 旋转校正算法的基础上，另在载体图像的中心处寻找某一固定安全区域，使得无论旋转角度大小，该处所提取的水印信息在受旋转攻击等几何攻击的干扰下具有较强的健壮性。

1.2.2 安全区域的确定

在人类视觉角度考量，当旋转角度为（45°、135°、225°和 315°）时，所选的区域（红框标注部分）刚好零损失；当角度超过 45°时，所选择的区域同样安全，所选择的区域不会受到旋转攻击而带来损失，故本文将所选择的区域叫做内接正方形安全区域。选取构建区域原理以及效果如图 5 所示。


(a) 校正旋转 45°


(b)构建正方形区域

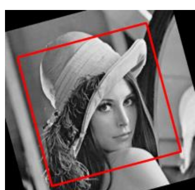

(c)标记所选的正方形

图 5　选取构建区域原理图以及效果

针对旋转攻击带来图像失真以及旋转校正后图像像素值缺失的问题，文献[10]利用伪 Zernike 矩的重构图像形成近似圆，但在像素选取以及分块处理相对麻烦，故本文选取内切正方形作为安全区域。对于内接正方形模长的选取问题，一方面，若该正方形区域的面积选取过大，会造成更多的像素缺损；另一方面，若选定面积选取过小，则会减少水印的容量。因此，为保证所提取的特征矩阵图像部分不受到损失且尽可能多的包含水印信息，本文将在受到损失面积最大的旋转校正后的图像中确定内接正方形的规模并保持边长度不变，使得即使在其他旋转角度下，该内接正方形区域内的像素点仍不发生变化。综上，在进行几何校正恢复后，构建载体内部像素稳定不变的正方形区域具有一定的可操作性。

为了验证所选的区域在受到旋转攻击时，安全区域内是否出现像素数据损失的现象，载体图像经过各种角度旋转攻击的效果（正常情况下内切正方形的规模）如图 6 所示。


(a) 旋转 5°


(b) 旋转 15°


(c) 旋转 30°


(d) 旋转 45°


(e) 旋转 55°

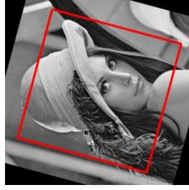
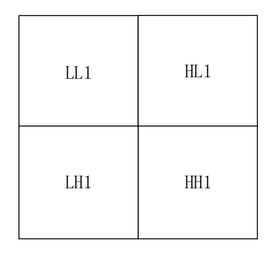

(f) 旋转 75 °

图 6　旋转攻击后选择区域缺损情况

1.3　冗余离散小波

由于冗余离散小波变换每进行下一级分解时所得的每个子图矩阵规模与原始图形矩阵规模一样，所以利用其特性不仅可以提取到图像稳定的低频区域，而且低频区域的矩阵规模会与原始图像保持一致，进而提高算法的鲁棒性和容量。二级 RDWT 分解示意图如图 7 所示。



(a) 一级 RDWT 分解

LL2　HL2
LH2　HH2　HL1
LH1　HH1

(b) 二级 RDWT 分解

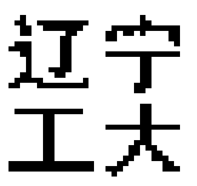
图 7　二级 RDWT 分解示意图

设图像矩阵 $A(m\times m)$，图像 A 经过一级 RDWT 分解得到一个低频信息，LL_1 表示图像的逼近部分，其矩阵大小为$(m\times m)$，LH_1、HL_1、HH_1 分别表示图像的垂直、水平和对角线方向的高频信息，三者表示图像的细节部分，其大小同样分别为$(m\times m)$。图 7(b)则是对 LL_1 进行下一级的 RDWT 分解，同理得到三个高频信息和一个低频信息，其矩阵大小保持不变。其中，小波分解级数越高，所得深层低频子带越集中包含了被分解图像的绝大部分信息。相比高频信息易受到噪声的攻击，低频子图抵抗外来影响因子能力较好，其稳定性较强。

与离散小波变换(discrete wavelet transform，DWT)相比，DWT 变换后所得到一级子图矩阵规模为原始图像矩阵的 1/4，而 RDWT 变换后子图矩阵规模不变，因此在水印算法容量角度上，RDWT 更具有优势，同样文献[11]也印证了应用在水印算法中 RDWT 比 DWT 具有更强的鲁棒性。因此选择 RDWT 变换后的低频子带信息，利用 SVD 进一步增加算法的稳定性和鲁棒性。

2　零水印的构建和水印提取

本文算法主要针对旋转校正后的相关水印算法进行优化，因此在旋转校正阶段在文献[5]的 SIFT 方法校正基础上，另增加了内接正方形安全区域确定理论。算法具体分为零水印的构建与水印的提取两个步骤。在构建零水印之前需要对水印进行 *Arnold* 置乱加密，以提高算法的安全性和鲁棒性。水印图像置乱后的效果如图 8 所示。



(a) 原始水印图像

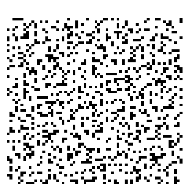

(b) 置乱后的水印图像

图 8　水印信息置乱前后的效果

2.1　零水印的构建流程

a) 对水印图像进行 *Arnold* 置乱，得到加密后的水印图像

$W(n \times n)$ 并保存秘钥 K。

b) 根据 1.2 节的讨论，确定载体图像中不会因受旋转攻击而导致像素缺失的内接正方形 $M(m \times m)$，其中 $mod(m,n)=0$，并保存内接正方形的左上角坐标以及边长。

c) 对 M 进行二级 RDWT 变换，提取其逼近子图并分块 $B_{i,j}$，其中，i,j=1,2,...m/n。

d) 对图像块进行 SVD 分解，并提取每个块的最大奇异值，构建过渡矩阵 Y。

e) 根据 Y 中元素值与其平均值 $mean_Y$ 的大小关系根据特征矩阵 C，如式(8)所示。

$$C(i,j)=\begin{cases}1 & Y(i,j)\ge mean_Y\\ 0 & Y(i,j)<mean_Y\end{cases} \tag{8}$$

f)将特征矩阵 C 与加密水印 W 进行异或操作，得到版权信息零水印 CW，并送至第三方权威机构认证中心(IPR)注册。

2.2　水印的提取

a)对可能受到旋转攻击的图像进行旋转判断与校正，得到待检测图像 P。

b)按照构建零水印的步骤 b)~e)，同理得到特征矩阵 C*。

c)从第三方权威机构认证中心获取零水印 CW，与特征矩阵进行异或操作，并提取秘钥 K 进行逆 Arnold 置乱，得到提取的水印图像 W*。

3　实验结果

仿真实验采用 MATLAB 2014a 作为实验平台，选取 6 幅纹理不同的灰度图像(512×512)，水印图像为 32×32 的带有“辽宁工大”标志的二值图像。其中置乱秘钥 K 为 20。本文采用误码率（*bit error ratio*，*BER*）和归一化相关系数（*normalized cross-correlation*，*NC*）来衡量提取到的水印图像与原始水印图像之间相近程度。*BER* 是指提取的水印错误的比特数占水印全部比特数的比例，这个值介于 0~1 之间，显然 *BER* 越接近于 0，水印的鲁棒性越好。*NC* 值的范围在 0~1 之间，且该值越接近于 1，表明该数字水印算法的鲁棒性越好。

BER 定义为

$$BER = N_{error} / N_{bits} \times 100(\%) \tag{9}$$

其中：N_{error} 表示与原始水印相比较，提取的水印信息中错误的比特值的个数；N_{bits} 表示水印中总的比特数。

NC 定义为

$$NC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{M} w(i,j)\times w^{*}(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{M} w(i,j)^{2}} \tag{10}$$

其中：$w(i,j)$ 为原始水印图像；$w^{*}(i,j)$ 为提取的水印图像；M 为水印图像的长或宽。

3.1　旋转攻击测试

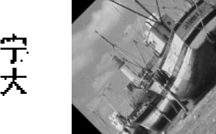
本节仅从以原始载体图像的中心点为旋转中心进行旋转攻击测试。对受到旋转攻击的载体图像，先进行 SIFT 特征点校正方法，然后选定安全区域，从而提取出水印信息。本测试实验将对 6 个不同的图像进行旋转攻击测试。

测试图像受到旋转攻击效果和提取的水印图像如图 9 所示，从不同载体图像受到不同旋转角度的攻击后提取的水印图像仍然清晰可见，而且从肉眼就可以进行版权的认证。

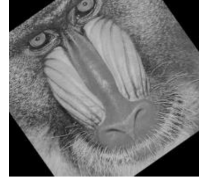
6 幅不同图像抵抗旋转攻击的 *NC* 值数据见表 2。从表 2 整体可得，当受到任意角度旋转攻击时，其提取到的水印 *NC* 值均在 0.996 2 以上，尤其当旋转 90° 时，其 *NC* 值均为 1。原因在于当图像受到 90° 旋转攻击时，图像无任何像素值缺损，而且 SVD 具有旋转不变性，所以 90° 的旋转攻击对水印的提取无影响；同理，当图像受到 180° 和 270° 的旋转攻击时，其提取到的 *NC* 值也为 1。



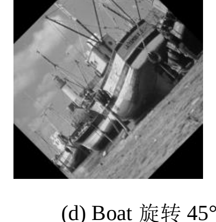
(a)Lena 旋转 15°



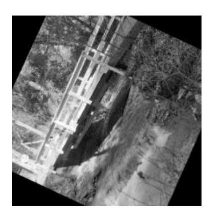
(b) Barbara 旋转 25°



(c) Baboon　旋转 35°



(d) Boat 旋转 45°



(e) Bridge 旋转 45°



(f) Couple 旋转 45°

图 9　测试图像受到旋转攻击效果和提取的水印图像

表 2　不同图像抵抗不同角度旋转攻击的 NC 值(逆时针旋转)

旋转角度(°)	Lena	Barbara	Baboon	Boat	Bridge	Couple
1	1.0000	0.9993	0.9987	1.0000	1.0000	0.9993
5	0.9974	0.9980	0.9993	0.9980	0.9993	0.9980
10	0.9974	0.9975	0.9955	0.9980	1.0000	0.9974
15	0.9980	0.9968	0.9955	0.9955	0.9993	0.9980
25	0.9993	0.9981	0.9948	0.9961	0.9987	0.9974
35	0.9980	0.9962	0.9929	0.9955	0.9993	0.9974
45	0.9974	0.9974	0.9942	0.9974	0.9993	0.9968
55	0.9993	0.9968	0.9968	0.9961	0.9993	0.9974
65	0.9980	0.9962	0.9942	0.9987	0.9980	0.9968
75	0.9980	0.9962	0.9968	0.9974	0.9993	0.9968
85	0.9980	0.9987	0.9974	0.9993	1.0000	0.9993
90	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
120	0.9980	0.9987	0.9935	0.9980	0.9987	0.9968

3.2 常规攻击测试

常规的攻击主要有几何攻击与非几何攻击，而在 3.1 节中已经讨论过本文算法抗旋转攻击的能力，因此在本节中不进行旋转攻击测试。取 6 幅常规图像中的 Lena、Barbara、Baboon 为例，其抵抗非几何攻击测试结果见表 3。

从表 3 中的数据可得，随着攻击强度的增加，提取水印的 *NC* 值逐渐减小，但减小速度缓慢，其整体最小 *NC* 值也在 0.95 以上。特别是针对 JPEG 压缩攻击，当 JPEG 压缩的质量因子为 1（压缩比为 100:100），从三幅不同的图像提取到的水印 *NC* 分别为 0.971 6，0.972 3 和 0.951 0，可见本文算法具有抵抗高强度 JPEG 压缩攻击的性能。同理，本文算法对其他类型攻击的效果也较为显著，均近似可得 1。

三幅图像受到不同几何攻击后提取水印的数据见表 4。其中，由于采用 SIFT 特征点的几何校正，使得算法能够有效地抵抗缩放攻击和行列偏移攻击，而且提取水印 *NC* 值均接近 1，具备良好的抗几何攻击能力。当受到剪切攻击时，由于剪切载体图像的 1/64 时，没有对提取图像特征点的区域造成影响，进而不会影响特征点的提取，从而使提取的水印非常完整，而当增加剪切面积时，会把部分提取特征点的区域减掉，直接影响了提取水印的质量，因此本文算法能够抵抗小范围的剪切攻击。

表 3　抵抗非几何攻击测试结果(NC 值)

攻击方式	参数	Lena	Barbara	Baboon
高斯噪声	0.010	0.9911	0.9903	0.9865
	0.020	0.9852	0.9858	0.9741
椒盐噪声	0.010	0.9968	0.9942	0.9948
	0.020	0.9923	0.9929	0.9923
JPEG	1	0.9716	0.9723	0.9510
	10	0.9974	0.9929	0.9832
	20	0.9936	0.9974	0.9916
中值滤波	3×3	0.9968	0.9968	0.9903
	5×5	0.9929	0.9923	0.9890
高斯低通滤波	3×3	0.9968	0.9980	0.9980
	5×5	0.9955	0.9968	0.9955
维纳滤波	3×3	0.9961	0.9987	0.9980
	5×5	0.9948	0.9955	0.9942
图像锐化	—	0.9916	0.9833	0.9871
直方图均衡化	—	0.9774	0.9872	0.9858

表 4　不同图像抵抗几何攻击测试结果(NC 值)

攻击方式	参数	Lena	Barbara	Baboon
缩放攻击	0.25	0.9923	0.9936	0.9929
	0.5	0.9980	0.9987	0.9974
	1.5	1.0000	1.0000	1.0000
剪切攻击	左上角 1/64	1.0000	1.0000	1.0000
	左上角 1/16	0.9871	0.9878	0.9656
循环偏移攻击	(50,50)	1.0000	1.0000	1.0000
	(100,0)	1.0000	1.0000	1.0000
	(0,100)	1.0000	1.0000	1.0000
	(128，128)	1.0000	1.0000	1.0000

3.3 对比实验测试

为了进一步体现本文算法抗旋转攻击的优越性，与文献[5,8,13]进行对比。其中文献[5]只采用了 SIFT 进行校正，却没有考虑旋转攻击给旋转校正后图像带来的损失；而后两种算法也仅考虑到了旋转却没有校正的问题，文献[8]采用 Gaussian-Hermite 确定局部不变区域构建特征矩阵，文献[13]通过计算图像归一化后的伪 Zernike 矩，然后选取部分合适的矩通过量化调制嵌入水印信息。从水印算法方面，文献[5]选择掩蔽性好的图像块作为嵌入子块，得到子块二级离散小波低频的左奇异矩阵，通过修改第一列元素间的大小关系来实现水印的嵌入；文献[13]计算图像归一化后的伪 Zernike 矩，然后选取部分合适的矩通过量化调制嵌入水印信息；而本文采用非嵌入式的零水印方法，不会给载体图像带来任何的视觉影响，因此本文具有较强的不可见性。不同文献方法下抗旋转攻击的对比实验数据见表 5。

表 5　不同文献的旋转攻击对比实验测试结果

旋转攻击角度/°	文献[5]	文献[8]	文献[13]	本文
0	1.0000	1.0000	1.0000	1.0000
10	0.9366	0.9867	0.9930	0.9974
20	0.8966	0.9820	0.9710	0.9993
30	0.8446	0.9855	0.9830	0.9980
40	0.7325	0.9822	0.9860	0.9987
50	0.7339	0.9820	0.9980	0.9980
60	0.8447	0.9873	0.9890	0.9961
70	0.8945	0.9865	0.9800	0.9987
80	0.9287	0.9898	0.9880	0.9947
90	1.0000	0.9901	1.0000	1.0000

由表 5 中的数据可分析，通过旋转校正优化后的水印算法抵抗旋转攻击的鲁棒性要明显优越于只进行校正的水印算法，其中文献[8,13]和本文算法属于旋转校正后选择合适的区域进行水印的提取，而文献[5]只进行旋转校正。文献[8]抵抗旋转攻击的平均 NC 值为 0.987 2，文献[13]抵抗旋转攻击的平均 *NC* 值为 0.988 8，本文抵抗旋转攻击的平均 *NC* 值为 0.998 1，可见本文算法抵抗旋转攻击的性能要略强与文献[8,13]。本文算法与文献[8]类似，都是选取局部区域嵌入有意义的二值水印图像，本文算法优于文献[8]的主要原因就是采用了图像矩阵的奇异值，图像矩阵的奇异值能够抵抗扰动干扰，能够有效抵抗旋转校正后，通过插值方式进行图像复原的干扰。而文献[13]虽然能够在一定程度上改善抵抗旋转攻击的鲁棒性，但其水印信息仅为长度为 128 的无任何意义的二值序列，且水印算法容量较小。

表 6　常规攻击对比实验提取水印的 NC 值

攻击方式	参数	文献[5]	文献[13]	本文算法
JPEG 压缩	20	0.9891	0.9840	0.9936
	10	0.9685	0.9070	0.9858

中值滤波攻击	3×3	0.9937	1.0000	0.9968
	5×5	0.9894	0.9670	0.9929
高斯噪声	0.01	0.9464	0.9500	0.9911
	0.02	0.8522	0.8400	0.9852
椒盐噪声	0.01	0.9623	1.0000	0.9968
	0.02	0.9350	0.9490	0.9923
缩放攻击	0.5	0.9988	0.9693	0.9981
	1.5	1.0000	1.0000	1.0000
循环平移	(50,50)	1.0000	1.0000	1.0000
	(100,0)	1.0000	1.0000	1.0000
	(0,100)	1.0000	1.0000	1.0000
	(128,128)	1.0000	1.0000	1.0000
剪切攻击	左上角 1/4	0.8661	0.9783	0.8488

对载体图像进行 JPEG 压缩攻击、噪声攻击和滤波攻击。以 Lena 图像为例，本文算法与文献[5,13]对受到不同攻击后提取水印的 *NC* 值见表 6。不同文献旋转攻击对比实验结果如图 10 所示。

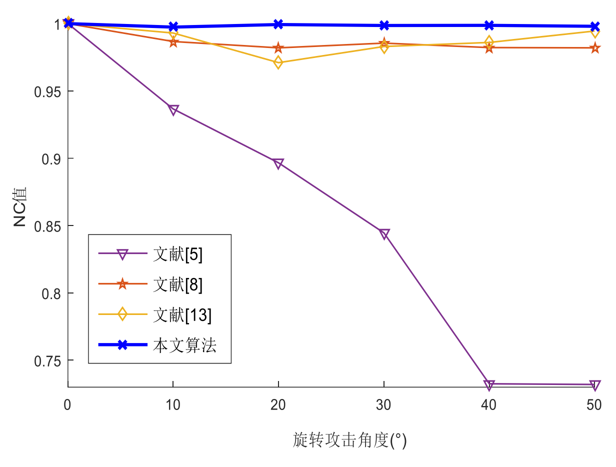


图 10　不同文献旋转攻击对比实验结果

由表 6 中可得，本文算法能够有效地抵抗 JPEG 压缩攻击、中值滤波攻击，高斯噪声攻击、椒盐噪声攻击、缩放攻击、循环平移攻击和剪切攻击。从受到不同程度 JPEG 压缩攻击后提取水印情况来看，本文算法提取水印的 *NC* 值的最小值仅为 0.985 8，最大值为 0.998 7，而文献[5,13]提取水印的 *NC* 值的最小值分别分 0.968 5 和 0.907 0，最大值均为 1，表明文献[13]算法抵抗 JPEG 压缩的能力衰减严重，其次是文献[5]，可见随着加重 JPEG 压缩攻击，本文算法抗 JPEG 压缩攻击的能力更加突出。尤其是抵抗噪声攻击，当受到 0.02 的高斯噪声攻击时，本文算法的鲁棒性比文献[5,13]分别高出了 15.61%和 17.29%；当受到 0.04 的椒盐噪声攻击时，本文算法的鲁棒性比文献[5,13]分别高出了 9.95%和 39.10%。同样从受到中值滤波攻击的数据来看，本文算法抵抗中值滤波攻击的能力也要优于文献[5,13]。对于缩放攻击与循环平移攻击，本文算法性能与文献[5,13]类似。但抗剪切攻击能力，本文算法不如文献[5,13]，其主要原因是本文算法在空域上进行嵌入区域的选择，当受到剪切攻击时，会有可能把所选择的区域减掉，使得提取水印的区域缺失，造成提取水印的不完整，但当受小面积的剪切攻击时，本文算法还是能够表现出良好的鲁棒性。

4　结束语

针对几何旋转攻击导致图像部分像素信息缺损无法提取完整水印的问题，本文提出了一种抗几何旋转校正后的图像优化零水印算法。原始载体图像预处理阶段，在 SIFT 法几何校正后，通过构建内接正方形安全区域，实现了在保证特征矩阵中所含像素信息无缺损下完成零水印的构建，恢复了水印的同步性。在零水印的构建和水印提取阶段，利用 RDWT 变换保留与原始图像矩阵规模同样大小的子图特性，提高了水印算法的容量；并利用低频信息和 SVD 的稳定特性来提高算法的鲁棒性。通过大量实验表明，算法能够有效地抵抗旋转攻击、缩放攻击、循环平移攻击以及剪切攻击，均体现了良好的鲁棒性。但在大面积地实现剪切攻击方面，本文算法能力仍有待提高。

参考文献：

[1] Wen Q, Sun T F, Wang S X. Concept and application of zero-watermark [J]. Acta Electronica Sinica, 2003, 31 (2): 214-216.

[2] 廖琪男. 基于 SIFT 特征点匹配的水印图像几何校正算法 [J]. 计算机应用研究, 2011, 28 (6): 2247-2249. (Liao Qinan. New watermarked image geometric correction algorithm based on SIFT feature points matching [J]. Application Research of Computers, 2011, 28 (6): 2247-2249.)

[3] 李浩，李宏昌. 一种基于 CS-SIFT 抗几何攻击的图像双水印算法 [J]. 计算机科学, 2014, 41 (S2): 263-267. (Li Hao, Li Hongchang. Geometric attack resisting double-watermarking algorithm based on CS-SIFT [J]. Computer Science, 2014, 41 (S2): 263-267.)

[4] 吕建平，彭述. 一种基于 SIFT 的 DWT 域抗几何攻击水印算法 [J]. 西安邮电大学学报，2015, 20 (02): 88-92. (Lyu Jianping, Peng Shu. A DWT-domain watermarking algorithm against geometric attacks based on SIFT [J]. Journal of Xi’an University of Posts and Telecommunications, 2015, 20 (2): 88-92.)

[5] 齐向明，高婷. 图像块的不可见性与鲁棒性均衡水印算法 [J]. 中国图象图形学报, 2017, 22 (6): 719-730. (Qi Xiangming, Gao Ting. Invisible and robust watermarking algorithm based on an image block [J]. Journal of Image and Graphics, 2017, 22 (6): 719-730.)

[6] 贾超，张政保. 基于改进 SIFT 的抗几何攻击水印算法 [J]. 小型微型计算机系统，2014, 35 (12): 2655-2658. (Jia Chao, Zhang Zhengbao. Resistance to geometric attacks watermarking algorithm based on improved SIFT [J]. Journal of Chinese Computer Systems, 2014, 35 (12): 2655-2658.)

[7] Zhang W, Chen J, Wang R, *et al.* Affine correction based image watermarking robust to geometric attacks [C]// Proc of IEEE International Conference on Parallel and Distributed Computing, Applications and

Technologies. 2017.

[8] Jia X, Yang Z, Qi Y, *et al*. The anti-geometric attack digital watermarking algorithm based on image normalization of local information [C]// Proc of IEEE Information Technology, Networking, Electronic and Automation Control Conference. 2016: 1120-1124.

[9] 朱丹丹，吕鲤志．基于伪 Zernike 矩和 Contourlet 变换的抗几何攻击图像水印算法 [J]．计算机科学，2016, 43 (6): 131-134. (Zhu Dandan, Lyu Lizhi. Anti-geometric-attack watermarking algorithm based on pseudo-zernike moments and contourlet transform [J]. Computer Science, 2016, 43 (6): 131-134.)

[10] 陈青，翁旭峰．基于 Harris 特征点和伪 Zernike 矩的鲁棒水印算法 [J]．电子科技，2016, 29 (3): 183-186. (Chen Qing, Weng Xufeng. A robust image watermarking based on harris feature points and pseudo-zernike moments [J]. Electronic technology, 2016, 29 (3): 183-186.)

[11] Rassem T H, Makbol N M, Khoo B E. Performance evaluation of RDWT-SVD and DWT-SVD watermarking schemes [C]// Proc of AIP Conference Proceedings. [S. l.] : AIP Publishing, 2016: 050021.

[12] Sun S, Yang S, Zhao L. Noncooperative bovine iris recognition via SIFT [J]. Neurocomputing, 2013, 120: 310-317.

[13] 陈青，翁旭峰．一种新的基于伪 Zernike 矩的图像盲水印算法 [J]．计算机应用研究，2016, 33 (9): 2810-2812. (Chen Qing, Weng Xufeng. Novel blind image watermarking based on pseudo Zernike moments [J]. Application Research of Computers, 2016, 33 (9): 2810-2812.)